Determinism vs. Probabilism, Introduction to Basic Methods and Structure of Probabilistic Risk Assessments (PRA)

Scope of Probabilistic Risk Assessment (PRA)

- Both accident initiating events and the unavailability of safety equipment or measures needed to handle accidents are assumed.
- The technical system and specific chains of events (scenarios) including their frequencies of occurrence and resulting plant states are modeled.
- Physical phenomena of the postulated scenarios are modelled, and respective consequences are assessed – inside and outside the plant.
- The risk of the analyzed system is the sum of the products of realistically identified consequences $x$ and their frequencies $h(x)$
  \[ R = x_1 \cdot h(x_1) + x_2 \cdot h(x_2) + \ldots \]
  for a representative number of exclusive initiating events and event chains.
Deterministic vs. probabilistic approach (1/2)

Deterministic (postulating)
- Events completely determined by cause-effect-chains (causality).
- Analyse of the effects of assumed causes.

Statistically (retrospective)
- Rules can be derived from a large number of similar events (based on experience).
- Directly applicable observations can be transferred to the system or to the event level.

Probabilistic (prognostic)
- Events can be identified by the probability of occurrence.
- Use of observations on the level of components (Axiom system of Kolmogoroff).

Deterministic vs. probabilistic approach (2/2)

Example „leakage of the primary coolant boundary“

Real leak spectrum (probabilistic)

Postulated (deterministic)

Break diameter

Probability (cumulative)
### Approaches

<table>
<thead>
<tr>
<th></th>
<th>Statistic</th>
<th>Deterministic</th>
<th>Probabilistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>a great number of similar events hold experiential values</td>
<td>events are completely predetermined through effect chains (causality)</td>
<td>Events can be identified through their probabilities of occurrence</td>
<td></td>
</tr>
</tbody>
</table>

### Methodology (within risk analyses)

<table>
<thead>
<tr>
<th></th>
<th>Statistic</th>
<th>Deterministic</th>
<th>Probabilistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyse of a great number of directly usable observations on the level of systems / events</td>
<td>Analyse of the effects of assumed causes on the level of relevant systems / events</td>
<td>Complete analyse of system caused event chains and realistic estimation of frequencies and consequences</td>
<td></td>
</tr>
<tr>
<td>(descriptive)</td>
<td>(definitive)</td>
<td>(prognostic)</td>
<td></td>
</tr>
</tbody>
</table>

### Risk definition

- risk = expected value \( \geq 0 \)
- risk = dependent probability

### Prerequisites

- Relative frequency
- Kolmogoroff axiom system

---

### Terms in the Field of Probabilistic Risk Assessments

- **Events (Examples):**
  - A pump fails within a defined time frame,
  - The wind speed exceeds a certain value within a defined time frame,
  - A great number of events cause physical reactions, etc.

- **Probabilities:**
  - Classical (Laplace): probability as the number of cases in which the event occurs, divided by the number of all possible cases (probability as relative frequency)
  - Frequency related (Mises): probability as a limiting value of the relative frequency of an event after a great (unlimited) number of repetitions under the same conditions.
  - Subjective: probability as a degree of the expectation or the confidence of an individual into a statement that a possible event occurs, a described circumstance occurs, etc.
Definition of some Terms

Absolute Frequency
- How often a given measured value occurs within a sample
  \( (\geq 0) \)

Relative Frequency
- Ratio between the number of certain events to the number of all events
  \( (\leq 1) \)

Probability
- Measure for the uncertainty of future events
  (between 0 and 1)

Frequency
- Time related frequency (e.g. number per year)
  \( (\geq 0) \)

Statistically

<table>
<thead>
<tr>
<th>Risk</th>
<th>expected value ( \geq 0 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( E(X) = \sum_{i=1}^{\infty} x_i \cdot \Pr(X=x_i) )</td>
<td>( \Pr(X) = \Pr(X</td>
</tr>
<tr>
<td>( \Pr(X): \text{ Expected value} )</td>
<td>( \Pr(E): \text{ Probability that a coin will be thrown} )</td>
</tr>
<tr>
<td>( X: \text{ Probability variable “heads”/“tails”} )</td>
<td>( \Pr(X</td>
</tr>
<tr>
<td>( \Pr(X</td>
<td>E) \cdot \Pr(E) = 0,5 \cdot 1 = 0,5 )</td>
</tr>
</tbody>
</table>

Probabilistically

<table>
<thead>
<tr>
<th>Observation: ( \sum_{i=1}^{\infty} x_i \cdot \Pr(X=x_i) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_i \cdot \Pr(X=x_i) )</td>
</tr>
<tr>
<td>( 0 \cdot 0,45 )</td>
</tr>
<tr>
<td>( 550 \cdot 0,55 )</td>
</tr>
<tr>
<td>( 1000 )</td>
</tr>
<tr>
<td>( 450 )</td>
</tr>
</tbody>
</table>

\( \Pr(X) = 0,55 \)

The „expectation” for „1” is closer to 100%

Axiom system of Kolmogoroff:
1. \( 0 \leq \Pr(A) \leq 1 \)
2. \( \Pr(\text{certain event}) = 1 \)
3. \[ \Pr(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \Pr(A_i) \]
Probabilistic Risk Assessments (PRA) in Comparison with Deterministic Approaches

- PRA as a complementary instrument.
- PRA aims at realistic description of risk and safety.
- PRA models provide information on expected performance of different safety measures; they disclose weak points.
- PRA reflects consequences of dependencies and man-machine interdependencies
- PRA shows uncertainties.
- PRA shows the relative importance of each accident sequence, it allows focusing on dominant accident sequences.
- PRA allows optimal allocation of available resources.

Structure and "Levels" of a PRA for Nuclear Power Plants

- **Level 1**: Frequency of core damage (CDF)
  - includes accident management measures
- **Level 2**: Frequency and amount of radionuclides released (source term, PDF)
- **Level 3**: Frequency and quantities of environmental and health effects
Initiating Events

Definition:
An initiating event is an incident which necessitates automatic or operator actions in order to bring the plant into safe steady state conditions; without such actions damage of the core may occur.

The tasks within a PRA level 1 are:
1. identification of the initiating events,
2. their classification into categories,
3. estimation of their frequencies.

Classification of initiating events

Plant internal initiating events
- Loss of Coolant Accidents
  - Breaks
  - Cracks/leakages
  - Wrong position of valves, et al.
- Transients
  - Increased heat production
  - Reduces heat removal

Plant external initiating events
- Earthquake
  - Airplane crash
  - Fire

Operation internal initiating events
- Internal fire
  - Internal flood et al.
Fault Tree Analysis I

Probability:
\[
P(Q) = P(A) + P(B) - P(A \cap B)
\]
\[
P(A) + P(B) - P(A \cap B)
\]

some conclusions:
1. A and B mutually exclusive:
   \[
P(A \cap B) = 0
   \]
   \[
P(Q) = P(A) + P(B)
   \]
2. A and B independent:
   \[
P(B | A) = P(B)
   \]
   \[
P(Q) = P(A) + P(B) - P(A) \cdot P(B)
   \]
3. A and B completely dependent:
   \[
P(B | A) = 1
   \]
   \[
P(Q) = P(A) + P(B) - P(A) = P(B)
   \]
   \[
P(Q) = P(A) + P(B)
   \]
always a conservative approach

Fault Tree Analysis II

Probability:
\[
P(Q) = P(A \cap B)
\]
\[
P(A) \cdot P(B | A) = P(B) \cdot P(A | B)
\]

some conclusions:
1. A and B independent:
   \[
P(B | A) = P(B)\] and
   \[
P(A | B) = P(A);
   \]
   \[
P(Q) = P(A) \cdot P(B)
   \]
2. A and B dependent:
   \[
P(Q) > P(A) \cdot P(B)
   \]
3. total dependence:
   \[
P(B | A) = 1
   \]
   \[
P(Q) = P(A)
   \]
approximations can be dangerous!
Fault Tree Analysis III

The systems fails (top event occurs), if cut sets
1. $A \cap B$
2. $A \cap B \cap C$
or minimal cut sets:
1. $A \cap B$
cut fail.

Flow Chart and its Fault Tree Representation
(simplified example)

- Top Event: Cooling System Fails
- No Water Supply
  - Operator Fails
- Flowmeter Fails
- Switch Fails
- Pumps Fails
- Emergency System Fails

CCF: Common Cause Failures
Construction of an event tree

Subsystem A Subsystem B  Subsystem... Final system state

Working, success  YES... 
Failure, collapse  NO...

Initiating event

Description: Leakage Fire Earthquake...

"After the failure of A the reaction B is stillok."

Description A, B, ...:
- Component, subsystem
- Human influence
- System, e.g., storage tank empty
- etc.

Description of system state:
- Systematic "Working"
- Failure chain
- Systematic "Explosion"
- Impact to the environment
- Evacuation, etc.

Pr = PrA (1-qK) (1-qB) (1-qD) (1-qE) (1-qF) (1-qG) (1-qH)

qi: dependent failure probability of a subsystem
PrA: probability of occurrence of the initiation event
Pr: probability of the complete path

Spring 2011 / Prof. W. Kröger

Application of an Event Tree in Nuclear Energy

"Large leakage in the primary loop" of a NPP

Complete function

\[ Pr = Pr_A (1-q_K) (1-q_B) (1-q_D) (1-q_E) (1-q_F) (1-q_G) (1-q_H) \]

q_i: dependent failure probability of a subsystem
PrA: probability of occurrence of the initiation event
Pr: probability of the complete path

Spring 2011 / Prof. W. Kröger
Divergences between event tree and fault tree analysis

<table>
<thead>
<tr>
<th>Fault tree</th>
<th>Event tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deductive</td>
<td>Inductive</td>
</tr>
<tr>
<td>Indicates the logic connection between events</td>
<td>Indicates the dependency of events which are set side by side (conditional probabilities)</td>
</tr>
<tr>
<td>A single chain of events from the “top event” to the basic event has no obvious importance (only sub fault trees)</td>
<td>All events along the chain from the initiating event to the final system state are of importance to the system</td>
</tr>
<tr>
<td>The system state at the knots aren’t indicated. The “top event” isn’t defining the system state (mostly the system failure)</td>
<td>Indicates many possible combinations of system/unit states and external events. The final state of a chain must be defined by the analyst.</td>
</tr>
<tr>
<td>Statical approach</td>
<td>Dynamic processes are taken into account</td>
</tr>
</tbody>
</table>

Overview of PRA methodology

[Diagram showing the steps of PRA methodology]

Initiating events (frequency) → Event tree/fault tree (probabilities with uncertainties) → Accident sequences (frequency) → Plant damage states → Accident progression/container failure events (probabilities with uncertainties) → Risk integration.

Various risk measures:

- Sensitivity analysis
- Reconsideration of very different sequences with high consequence
Characterization of a full PRA

Example: KKL, KKM

- Up to 100 initiating events (power operation + shut down states)
- Millions of accident sequences added to a total core damage frequency (CDF); combined use of fault tree and event tree techniques
- 8,000 sequences (≥10-10 a⁻¹) binned into 20 plant damage states (PDS)
- 15 to 20 release categories and 10 to 15 damage indicators per release category formed